PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/08, 19/00, 7/10

A2

(11) International Publication Number: WO 98/14915

(43) International Publication Date: 9 April 1998 (09.04.98)

(21) International Application Number: PCT/CA97/00717

(22) International Filing Date: 30 September 1997 (30.09.97)

(30) Priority Data:

60/027,781	1 October 1996 (01.10.96)	US
08/821,732	20 March 1997 (20.03.97)	US

(71) Applicant: OMEGA DIGITAL DATA INC. [CA/CA]; 8100 Keele Street, Concord, Ontario L4K 2A3 (CA).

(72) Inventor: COVELEY, Michael; 6 Fairview Avenue, Richmond Hill, Ontario L4C 6L2 (CA).

(74) Agents: RUSTON, David, A. et al.; 6th floor, 330 University Avenue, Toronto, Ontario M5G 1R7 (CA).

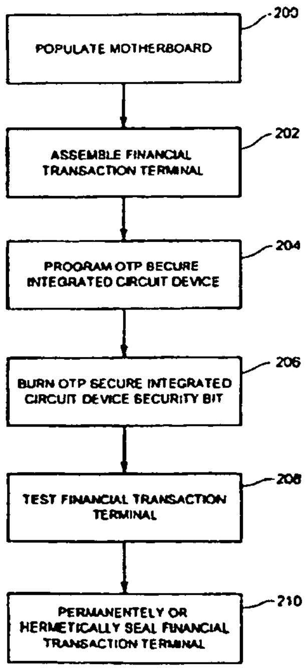
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: A METHOD OF ASSEMBLING AND PROGRAMMING A SECURE PERSONAL IDENTIFICATION NUMBER ENTRY DEVICE

(57) Abstract

A method of assembling and programming a secure personal identification number entry device is disclosed whereby the secure personal identification number entry device is programmed with security software including an encryption algorithm by way of an external port on the secure personal identification number entry device after the secure personal identification number device has been fully assembled.


200
POPULATE MOTHERBOARD
202
ASSEMBLE FINANCIAL TRANSACTION TERMINAL
204
PROGRAM OTP SECURE INTEGRATED CIRCUIT DEVICE
206
BURN OTP SECURE INTEGRATED CIRCUIT DEVICE SECURITY BIT
208
TEST FINANCIAL TRANSACTION TERMINAL
210
PERMANENTELY OR HERMETICALLY SEAL FINANCIAL TRANSACTION TERMINAL

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

A METHOD OF ASSEMBLING AND PROGRAMMING A SECURE PERSONAL IDENTIFICATION NUMBER ENTRY DEVICE

TECHNICAL FIELD

The present invention relates to secure personal identification number entry devices such as point-of-sale financial transaction terminals and in particular to a method of assembling and programming a secure personal identification number entry device.

BACKGROUND ART

Financial transaction terminals to read data stored on credit, debit and/or smart cards to complete financial transactions are known. Existing terminals such as automated banking machines (ABM's) require users to walk to a central retail platform to complete a financial transaction. More recently point-of-sale debit card terminals have been developed which allow a user to enter remotely their personal identification number (PIN) into a secure PIN entry device (SPED) together with a financial transaction request after their credit, debit or smart card has been read to access their account at a financial institution and withdraw funds directly to complete the financial transaction.

In order to maintain security, multi-digit PINs are used which are known only to the users and to the financial institutions issuing the debit, credit or smart cards. When a PIN is entered into the SPED by a user, the SPED encrypts the PIN via security software before transmitting the encrypted PIN to the financial institution together with the financial transaction request. Encrypting the PIN substantially reduces the risk of the PIN becoming known to other parties.

Conventional SPEDs typically include a tamper resistant casing which is either hermetically sealed or uses one way screws so that access to the internal components of the SPED cannot be achieved without physical evidence. The security software which includes the cryptographic keys and encryption algorithms used by the SPED is stored in a secure manner using a single integrated circuit design having on-board memory.

In order to maximize security, the SPED security software must be protected to inhibit access to and/or alteration of the encryption algorithms. This can be achieved by using a mask programmed device or a one-time programmable (OTP) device.

Mask programmed devices provide a good solution only if the encryption algorithms and SPED system software are identical for large groups of financial institutions and card issuers. Unfortunately, the encryption algorithms used by the financial institutions and card issuers differ for each type of card and from country to country. Moreover, the encryption algorithms tend to change as each financial institution develops improvements to the encryption algorithms to improve security. These differences in SPED operating software make the use of mask programmed devices unsuitable.

In contrast, OTP devices provide greater flexibility allowing the SPED security and system software to be tailored for each specific financial institution and/or card issuer. During the manufacture of conventional SPEDs incorporating OTP devices, the OTP devices are firstly programmed with the SPED system and security software. The OTP devices are then burned with a security bit. Following this, the printed circuit board (PCB) within the SPED is populated with its internal electronic components including the programmed OTP device and the SPED is fully assembled. Following this, the SPED is tested and if the results of the tests are satisfactory, the SPED casing is permanently or hermetically sealed.

The above manufacturing process is usually performed for specific customers and in ordered quantities and only after the purchase of the components of the SPED. Component programming lead times must therefore be taken into account for the OTP device programming steps thereby increasing the SPED manufacturing process time. Accordingly, improved methods of assembling and programming SPEDs are desired.

It is therefore an object of the present invention to provide a novel method of assembling and programming a secure personal identification number entry device such as a point-of-sale financial transaction terminal.

DISCLOSURE OF THE INVENTION

Broadly stated, the present invention provides a novel method of assembling and programming a secure personal identification number entry device (SPED) which allows the printed circuit board within the SPED to be populated in large batches. In one embodiment, the method includes the steps of populating a printed circuit board with the internal electronic components of the SPED including the OTP secure integrated circuit device and then assembling the SPED. Once assembled, the OTP secure integrated circuit device on the printed circuit board is programmed with the SPED system and security software by way of an external serial port on the SPED. Following this, the SPED is burned with a security bit and the SPED is tested. After testing, the SPED is permanently or hermetically sealed to inhibit access to the fully programmed OTP secure integrated circuit device within the SPED.

In another embodiment, the method includes the step of programming the OTP secure integrated circuit device with the SPED system software, test function software and a security software applications interface. The SPED printed circuit board is then populated with the internal electronic components of the SPED including the OTP secure integrated circuit device and the SPED is assembled. Once assembled, the SPED is tested and then permanently or hermetically sealed. After permanently or hermetically sealing the SPED, the OTP secure integrated circuit device is programmed with the SPED security software and is then burned with the security bit by way of an external serial port.

According to one aspect of the present invention there is provided a method of assembling and programming a secure personal identification number entry device, said secure personal identification number entry device including an outer casing, input means on said casing to allow financial transaction data including a personal identification number or a password to be entered therein, a card reader accommodated by said outer casing to receive and read a credit, debit or smart card, a processor within said outer casing and in communication with said input means and card reader, said processor including a one-time programmable secure integrated circuit device to encrypt said personal identification number or password and a transmitter to transmit said financial transaction data including the encrypted personal identification number or password to a financial institution for processing, said method comprising the steps of:

(i) populating a printed circuit board with electronic components forming said processing means including said one-time programmable secure integrated circuit device;

(ii) assembling said secure personal identification number entry device; and

(iii) programming said one-time programmable secure integrated circuit device with security software including an encryption algorithm by way of an external port on said outer casing.

According to another aspect of the present invention there is provided a secure personal identification number entry device comprising:

an outer casing;

input means on said outer casing to allow financial transaction data including a personal identification number or password to be entered therein;

a card reader accommodated by said outer casing.to receive and read a credit, debit or smart card;

a processor within said outer casing and in communication with said input means and said card reader, said processor including a one-time programmable secure integrated circuit device to encrypt said personal identification number or password;

a transmitter to transmit said financial transaction data including the encrypted personal identification number or password to a financial institution for processing; and

an external port on said outer casing electrically connected to said processor to allow said one-time programmable secure integrated circuit device to be programmed with security software after assembly of said secure personal identification number entry device.

According to still yet another aspect of the present invention there is provided in a method for assembling and programming a secure personal identification number entry device to generate a financial transaction request from entered financial transaction data including an encrypted personal identification number or password, the improvement comprising the step of:

(i) programming said secure personal identification number entry device with security software including an encryption algorithm by way of an external port on said secure personal identification number entry device after said secure personal identification number entry device has been assembled.

The present invention provides advantages in that manufacturing lead times due to programming operations are reduced while increasing security and maintaining high programming flexibility.

BRIEF DESCRIPTION OF THE DRAWING

Embodiments of the present invention will now be described more fully with reference to the accompanying drawings in which:

Figure 1 is a schematic representation of a financial transaction system;

Figure 2 is a perspective view of a portable, radio frequency financial transaction terminal utilized in the financial transaction system of Figure 1;

Figure 3 is a top plan view of the radio frequency financial transaction terminal of Figure 2;

Figure 4 is a block diagram of the radio frequency financial transaction terminal of Figure 2;

Figure 5 is a block diagram of a secure integrated circuit device forming part of the radio frequency financial transaction terminal of Figure 2;

Figure 6 is a block diagram of a central network controller forming part of the financial transaction system of Figure 1;

Figure 7 is a flow chart setting forth the steps by which the portable, radio frequency financial transaction terminal of Figure 2 is programmed and assembled; and

Figure 8 is a flow chart setting forth an alternative embodiment of the steps by which thc portable radio frequency financial transaction terminal is programmed and assembled.

BEST MODE FOR CARRYING OUT THE INVENTION

Referring now to Figure 1, a financial transaction system is shown and is generally indicated to by reference numeral 10. Financial transaction system 10 includes a central network controller 12 and a plurality of secure personal identification number entry devices (SPEDs) in the form of portable, hand-held, radio frequency (RF) financial transaction terminals 14. The central network controller 12 and the RF financial transaction terminals 14 communicate via a wireless RF communications link 16. The central network controller 12 also communicates with host computers at financial institutions (not shown) either via hardwired network services (i.e. DATAPAC), an ISDN interface or alternatively a wireless communications network to provide real-time financial transaction processing with the host computers.

Each RF financial transaction terminal 14 includes a financial transaction data module 18 for collecting financial transaction data and an RF transceiver 20 for transmitting a financial transaction request to the central network controller and for receiving a financial transaction verification from the central network controller 12. The RF transceiver is in the form of an RF modem having an internal microcontroller unit (MCU) and an antenna.

Referring now to Figures 2 to 4, one of the RF financial transaction terminals 14 is better illustrated. The RF financial transaction terminal includes a portable, hand-held outer casing 30 which accommodates the various components of the financial transaction data module 18 and the RF transceiver 20. The outer casing 30 includes a top casing shell 30a and a bottom casing shell 30b secured together by one way screws 32 so that once assembled, access to the interior of the financial transaction terminal 14 cannot be achieved without physical evidence. A retractable, pistol-grip handle 34 is received in a recess 36 formed in the undersurface of the bottom casing shell 30b and is retained by a plurality of fasteners 38 in the form of screws. A rechargeable battery 40 is received by a pocket (not shown) in the bottom casing shell. A multi-pin universal serial port 42 to connect to an optional bar code reader, CCD scanner or other similar device (not shown) is also provided in the bottom casing shell 30b and is hidden by a sliding cover 44. An auxiliary secure RS-232 serial port 94 (see Figure 4) is also provided on the side of the outer casing 30.

On the top casing shell 30a is an LCD display 50 and an input keypad 52 to allow financial transaction data to be entered into the financial transaction terminal and displayed. Above the LCD display 50 is a printer 54 housing a paper roll to print receipts confirming that financial transactions have been verified and processed. A card reader 56 having a card reading slot 58 therein is housed by the outer casing 30 adjacent one end thereof. The antenna 60 forming part of the RF transceiver 20 is rotatably mounted on the outer casing 30. Details of the antenna design are described in Applicant's co-pending application entitled "Rotatable Antenna for Financial Transaction Terminal" filed on even date herewith.

Within the outer casing 30 is a motherboard on which the internal components of the financial transaction terminal are mounted. In particular, the financial transaction terminal includes a main central processing unit (CPU) module 70 which communicates with a secure module 72. The functional division of the internal components into the main CPU module 70 and the secure module 72 is chosen for security.

The main CPU module 70 includes a printer interface 74 to connect to printer 54, an RF TX-RX interface 76 to connect to RF modem 20, a card reader interface 78 to connect to card reader 56 and a bar code reader interface 80 connected to universal serial port 42. The main CPU module 70 is also equipped with a main CPU 82 connected to the interfaces allowing the CPU to control the operation of the printer, the RF modem, the card reader and the device connected to the universal serial port 42. The CPU 82 is also connected to flash memory 84 and static random access memory 86. The flash memory 84 stores start-up software incorporating a set of routines for initializing the RF financial transaction terminal 14 at power-up. The flash mcmory 84 also stores a system software loader comprising a routine for downloading system software into thc flash memory 84. Flash memory 84 stores the system software (i.e. interrupt handlers, I/O routines, an application software loader, device drivers etc.) and an applications program area or memory space where a secure prompt table and different application programs can be downloaded (i.e. transaction verification, application specific services etc.) A photosensor 88 is also provided in the main CPU module 70 for security purposes as will be described and is connected to the secure module 72.

The secure module 72 provides cryptographic services and security measures to protect the RF financial transaction terminal 14 from software tampering that could result in debit, credit or smart card PINs or passwords from being accessed. The secure module 72 contains a microcontroller unit in the form of a physically encapsulated, one-time programmable (OTP) secure integrated circuit device 90 which controls the operation of the LCD display 50, the keypad 52 and a speaker 92 by way of display, keypad and speaker interfaces 110, 108 and 112 respectively. The secure integrated circuit device 90 also controls an auxiliary secure RS-232 serial port 94 and an interface 96 to the main CPU module 70. Auxiliary secure serial port 94 allows updates to data and software used by the financial transaction terminal 14 to be downloaded. The main CPU module 70 and the secure module 72 receive power from the on-board rechargeable battery 40 in a conventional manner.

The secure integrated circuit device 90 includes a CPU 100, read only memory 102 and random access memory 104. The read only memory 102 stores system software for auxiliary secure RS-232 port control, display control, control of communications to the main CPU module 70, keypad control and speaker control functions. The random access memory 104 is used for cryptographic key and encryption algorithm storage, PIN or password storage and system software and security software working space. The secure module 72 controls the LCD display 50 in a split-screen fashion dividing the LCD display into unsecured and secure display areas. The information displayed in the secure display area is controlled solely by the secure module 72 while the information displayed in the unsecured display area is controlled by the secure module in conjunction with the main CPU module 70.

A battery backup 120 is provided to protect against inadvertent power loss and consequent loss of data stored in the static random access memory 86 and random access memory 104 in which the cryptographic keys and encryption algorithms are stored. Read only memory 104 is designed so as to prevent unauthorized reading of its contents. In addition, since the photosensor 88 is within the outer casing 30, it is typically isolated from light. However, if the integrity of the outer casing 30 is compromised and the interior of the casing is exposed to light, the photosensor 88 triggers the secure integrated circuit device 90 which in turn clears the cryptographic keys and encryption algorithms stored in the random access memory 104 to inhibit an intruder from acquiring the cryptographic keys and encryption algorithms.

Referring now to Figure 6, the central network controller 12 is better illustrated. The central network controller in this embodiment is connected to a dial-up or leased-line telephone line and is powered by a power supply connected to AC mains. The central network controller includes a CPU motherboard with a main microprocessor 132 and associated memory 134. The main microprocessor 132 is connected to an RF transceiver including an RF modem 136 and an antenna 138 for establishing the RF communications link 16 with the various financial transaction terminals 14. A network interface 140 is provided with DATAPAC 3101 and 3201 surface or other similar interfaces. An ISDN interface board may also be provided. A serial RS-232 interface 142 is included in the central network controller 12 to allow updates to data and software used by the financial transaction terminals 14 and central network controller 12 to be downloaded. A serial RS-485 interface 144 is also provided for optional connection of the central network controller 12 to a retailer's existing point-of-sale platforms

In operation, financial transactions are carried out by bringing one of the financial transaction terminals 14 to the location of a user. Transaction data is entered into the financial transaction terminal via the input keypad 52 and displayed via LCD display 50. The user's debit, credit or smart card is read by the card reader 56 in the financial transaction terminal in the presence of the user. The user is required to enter a PIN or password via the keypad 52. The financial transaction terminal 14 does not display the entered PIN or password data or the data read by card reader 56. The secure integrated circuit device 90 encrypts the PIN or password data to inhibit the data from being accessed by unauthorized parties. Once encrypted, a financial transaction request is generated by the financial transaction terminal 14 which includes the financial transaction data i.e., the entered transaction data, read card data and encrypted PIN or password). The financial transaction request is then transmitted to the central network controller 12 by the RF modem 20 over the RF communications link 16.

The central network controller 12 in turn conveys the financial transaction request to the financial institution so that the financial transaction can be verified and processed. Once verified processed, the financial institution conveys verification data to the central network controller 12. The central network controller in turn transmits the verification data to the financial transaction terminal 14 to inform the user that the financial transaction has been verified and processed. The financial transaction terminal in turn prints a receipt confirming that the transaction has been verified and processed. Further details of the operation of the financial transaction terminals and central network controller are described in Applicant's co-pending PCT application serial No. PCT/CA96/00104 filed on February 22, 1996 and designating the United States, the content of which is incorporated herein by reference.

When manufacturing a financial transaction terminal 14, it is necessary to populate the motherboard with the internal components of the financial transaction terminal, program the main central processing unit module 70 and secure module 72, test the financial transaction terminal 14 and then permanently seal the outer casing 30 so that physical tampering with the financial transaction terminal is visible.

To reduce manufacturing costs, it is preferred that the financial transaction terminals are manufactured in large batches. In order to reduce further manufacturing costs, each financial transaction terminal is assembled and programmed in the following manner as will now be described with particular reference to Figure 7. Initially, the motherboard is populated with the internal components of the financial transaction terminal (step 200) and the financial transaction terminal is fully assembled (step 202). Once assembled, the secure integrated circuit device 90 is programmed with the operating system comprising the system software and the security software which includes the encryption algorithms and the cryptographic keys (block 204). The secure integrated circuit device 90 is then burned with a security bit (block 206). Steps 204 and 206 are performed by way of universal serial port 42, interface 80 and main CPU 82. Once the secure integrated circuit device 90 has been programmed, the financial transaction terminal is tested (step 208) and if the results of the tests are satisfactory, the outer casing 30 is permanently sealed (block 210) to inhibit access to the fully programmed secure integrated circuit device within the financial transaction terminal 14.

As those of skill in the art will appreciate, because the financial transaction terminal can be programmed with the operating system after the financial transaction terminal has been assembled, manufacturing lead times due to programming steps during assembly of the financial transaction terminal can be avoided.

Referring now to Figure 8, another method of assembling and programming each financial transaction terminal is shown. In this method, the secure integrated circuit device 90 is initially programmed with generic system software, test function software and a security software applications interface (step 300). The motherboard is then populated with the internal components of the financial transaction terminal (step 302) and the financial transaction terminal 14 is fully assembled (step 304). Once assembled, the financial transaction terminal is tested (step 306) and is then permanently sealed (step 308). After this, the secure integrated circuit device 90 is programmed with the encryption algorithms and the cryptographic keys (step 310). The secure integrated circuit device is then burned with a security bit (block 312). Steps 310 and 312 are performed by way of universal serial port 42, interface 80 and main CPU 82 to inhibit access to the fully programmed secure integrated circuit device within the financial transaction terminal. Since the secure integrated circuit device 90 is programmed with the security software after the financial transaction terminal is permanently sealed, the financial institutions can tailor the security features to their specific requirements by verifying the security code checksums, programming the secure integrated circuit device and burning the security bit, all in their own secure environments. This assembly and two-step programming approach for the financial transaction terminal reduces manufacturing lead-times to programming operations and provides for good security with excellent flexibility.

Although the present invention has been described with particular reference to radio frequency financial transaction terminals, it should be apparent to those of skill in the art that the methodology used to assemble and program the financial transaction terminals is equally applicable to stand-alone secure PIN entry devices, integrated point-of-sale devices and other secure PIN entry systems.. It should also be appreciated that various modifications and variations may be made to the present invention without departing from the spirit and scope thereof as defined by the appended claims.

<u>What is claimed is</u>:

1. A method of assembling and programming a secure personal identification number entry device, said secure personal identification number entry device including an outer casing, input means on said casing to allow financial transaction data including a personal identification numbers or a password to be entered therein, a card reader accommodated by said outer casing to receive and read a credit, debit or smart card, a processor within said outer casing and in communication with said input means and card reader, said processor including a one-time programmable secure integrated circuit device to encrypt said personal identification number or password and a transmitter to transmit said financial transaction data including the encrypted personal identification number or password to a financial institution for processing, said method comprising the steps of:

(i) populating a printed circuit board with electronic components forming said processing means including said one-time programmable secure integrated circuit device;

(ii) assembling said secure personal identification number entry device; and

(iii) programming said one-time programmable secure integrated circuit device with security software including an encryption algorithm by way of an external port on said outer casing.

2. The method of claim 1 further comprising the steps of testing said secure personal identification number entry device and if the results of the tests are satisfactory, permanently or hermetically sealing said outer casing.

3. The method of claim 2 wherein said testing and sealing steps are performed after step (iii).

4. The method of claim 2 wherein during step (iii) said one-time

programmable secure integrated circuit device is also programmed with system software.

5. The method of claim 2 wherein said testing and sealing steps are performed after step (ii) and prior to step (iii).

6. The method of claim 5 wherein prior to step (i), said one-time programmable secure integrated circuit device is programmed with system software.

7. A secure personal identification number entry device comprising:

an outer casing;

input means on said outer casing to allow financial transaction data including a personal identification number or password to be entered therein;

a card reader accommodated by said outer casing to receive and read a credit, debit or smart card;

a processor within said outer casing and in communication with said input means and said card reader, said processor including a one-time programmable secure integrated circuit device to encrypt said personal identification number or password;

a transmitter to transmit said financial transaction data including the encrypted personal identification number or password to a financial institution for processing; and

an external port on said outer casing electrically connected to said processor to allow said one-time programmable secure integrated circuit device to be programmed with security software after assembly of said secure personal identification number entry device.

8. A secure personal identification number entry device as defined in claim 7 wherein said external port is a RS-232 serial port.

9. In a method for assembling and programming a secure personal identification number entry device to generate a financial transaction request from entered financial transaction data including an encrypted personal identification number or password, the improvement comprising the step of:

(i) programming said secure personal identification number entry device with security software including an encryption algorithm by way of an external port on said secure personal identification number entry device after said secure personal identification number entry device has been assembled.

10. The method of claim 9 further comprising the step of permanently or hermetically sealing said secure personal identification number entry device after step (i).

11. The method of claim 10 further comprising the step of permanently or hermetically sealing said secure personal identification number entry device prior to step (i).

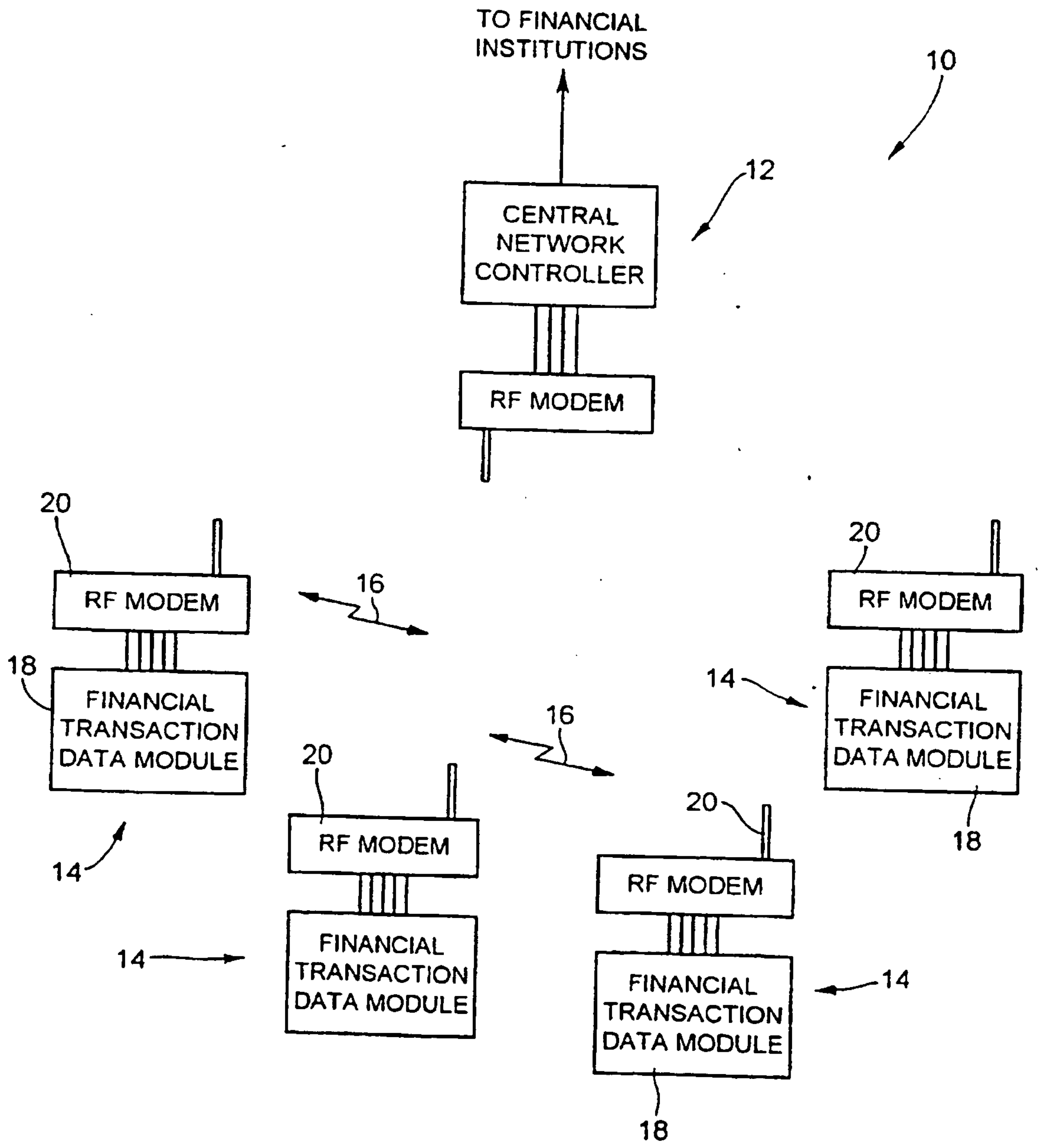

TO FINANCIAL INSTITUTIONS
10
12
CENTRAL NETWORK CONTROLLER
RF MODEM
20
RF MODEM
16
18
FINANCIAL TRANSACTION DATA MODULE
14
20
RF MODEM
FINANCIAL TRANSACTION DATA MODULE
14
16
20
RF MODEM
14
FINANCIAL TRANSACTION DATA MODULE
18
20
RF MODEM
FINANCIAL TRANSACTION DATA MODULE
14
18

FIG. 1

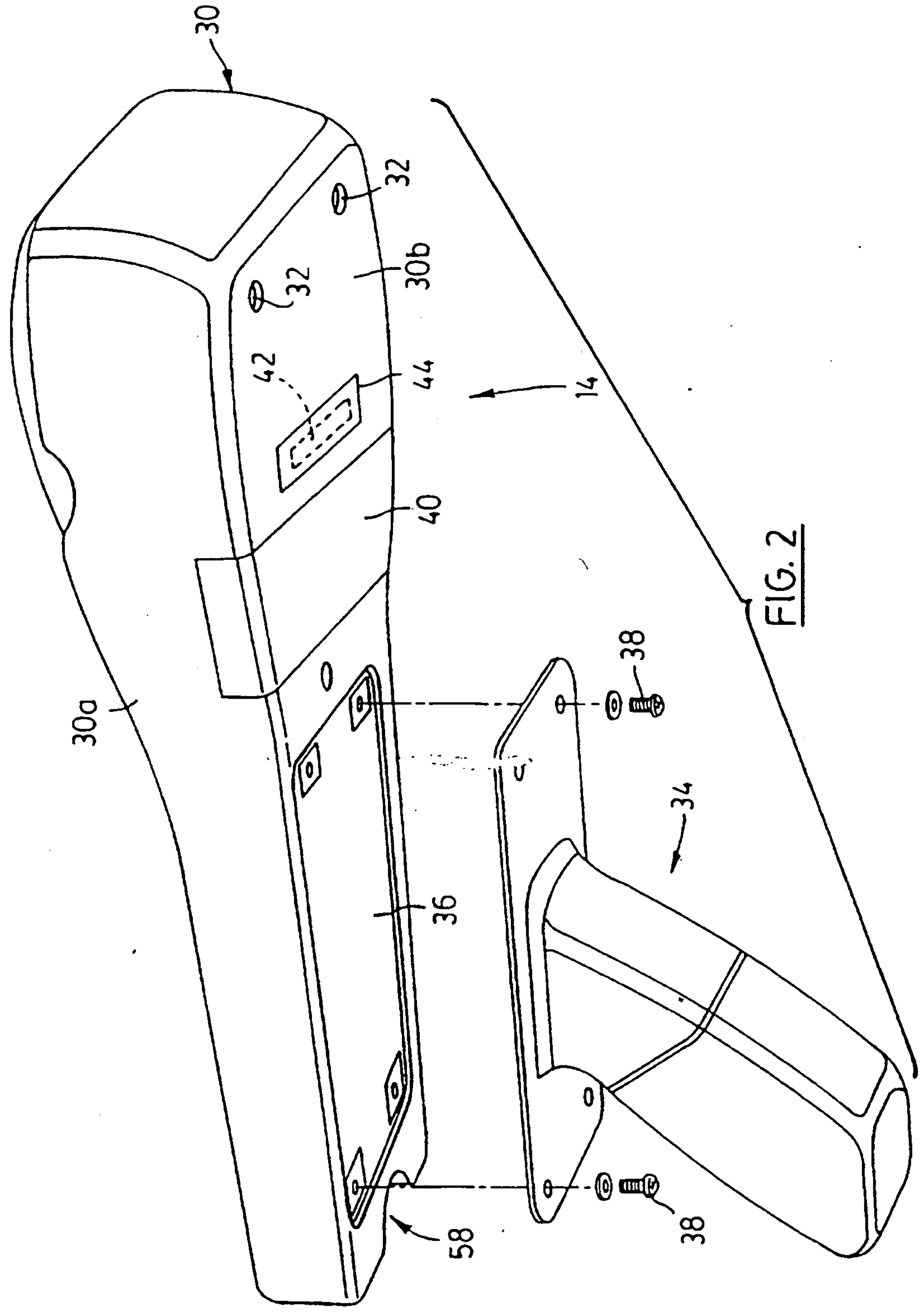


FIG. 2

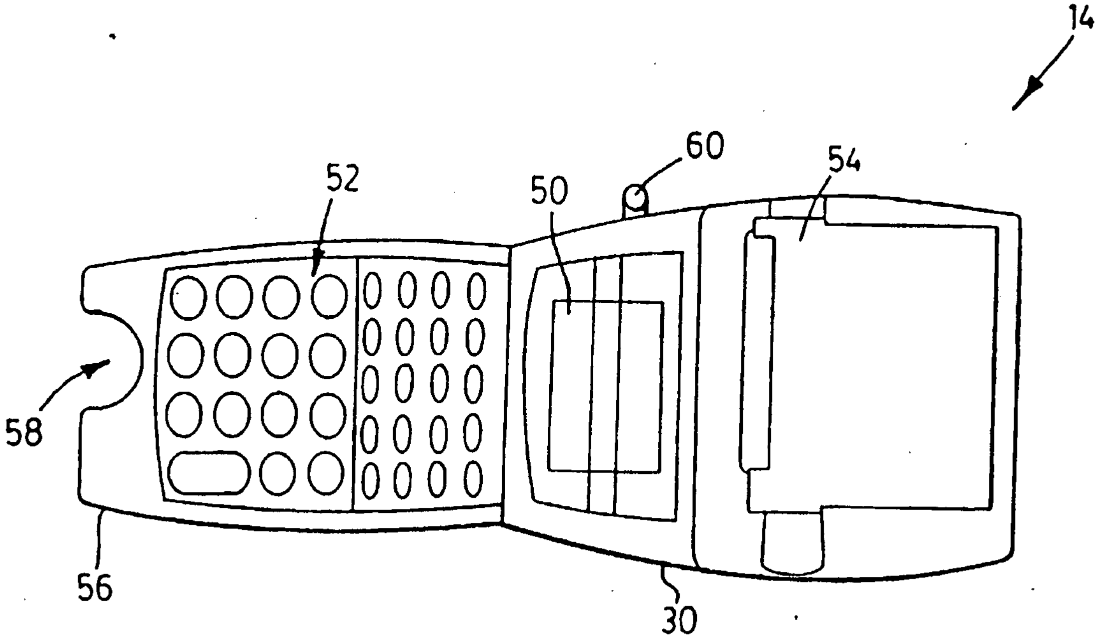


FIG.3

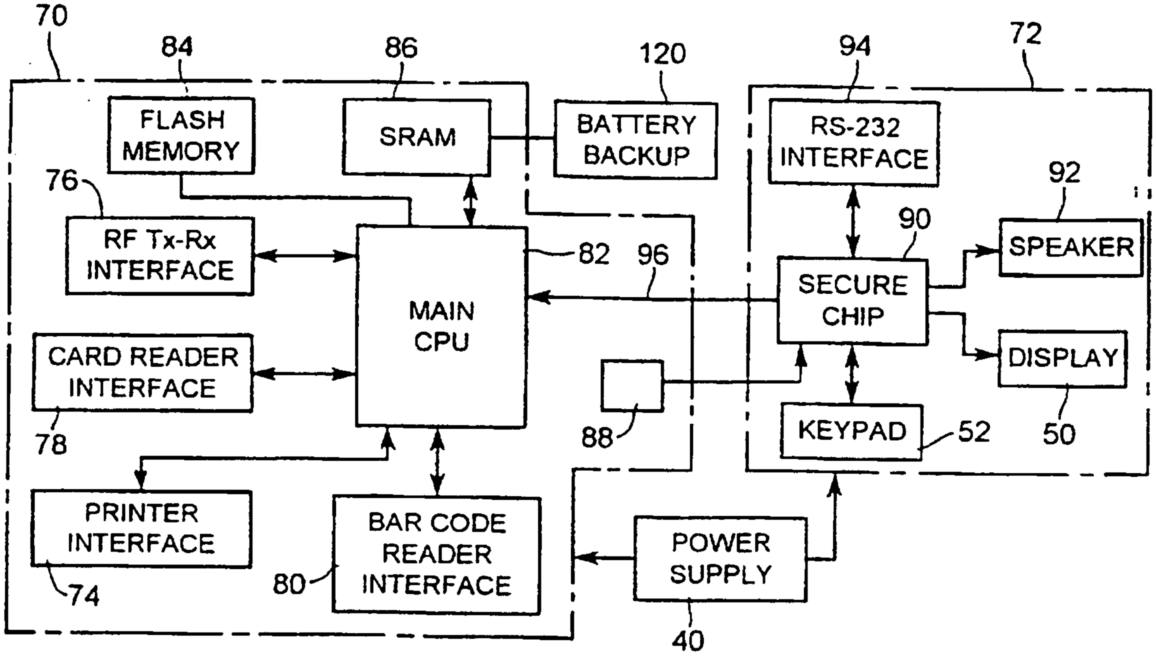

70
84
86
120
94
72
FLASH MEMORY
SRAM
BATTERY BACKUP
RS-232 INTERFACE
76
RF Tx-Rx INTERFACE
MAIN CPU
82
96
90
92
SECURE CHIP
SPEAKER
DISPLAY
CARD READER INTERFACE
78
88
KEYPAD
52
50
PRINTER INTERFACE
74
80
BAR CODE READER INTERFACE
POWER SUPPLY
40

FIG. 4

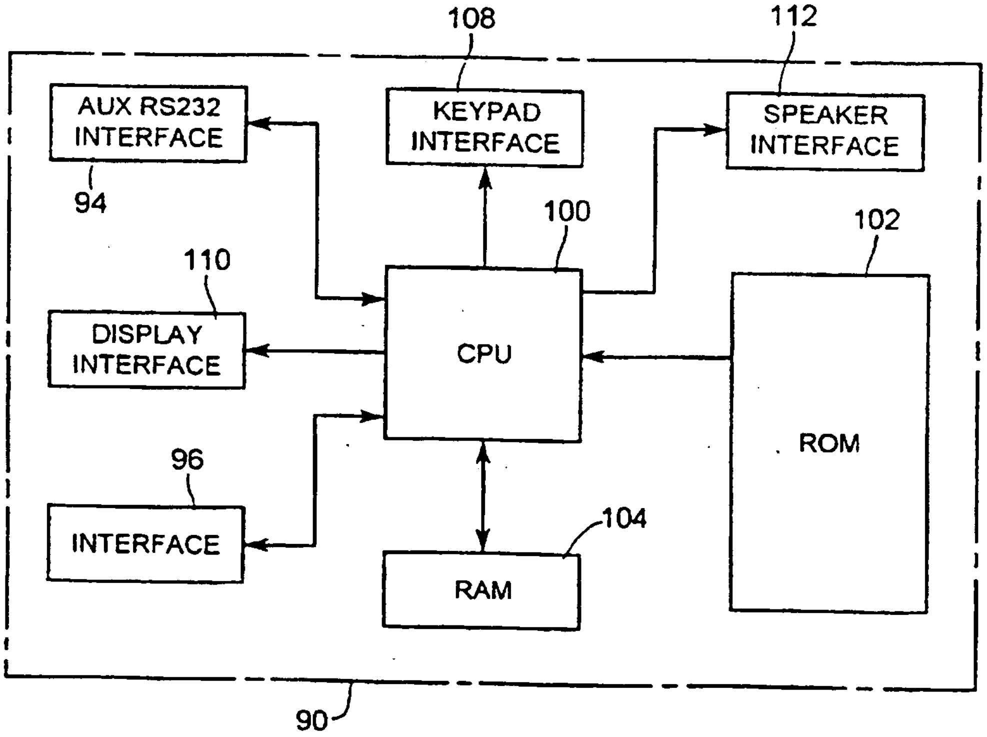

108
112
AUX RS232 INTERFACE
KEYPAD INTERFACE
SPEAKER INTERFACE
94
100
102
110
DISPLAY INTERFACE
CPU
ROM
96
INTERFACE
104
RAM
90

FIG. 5

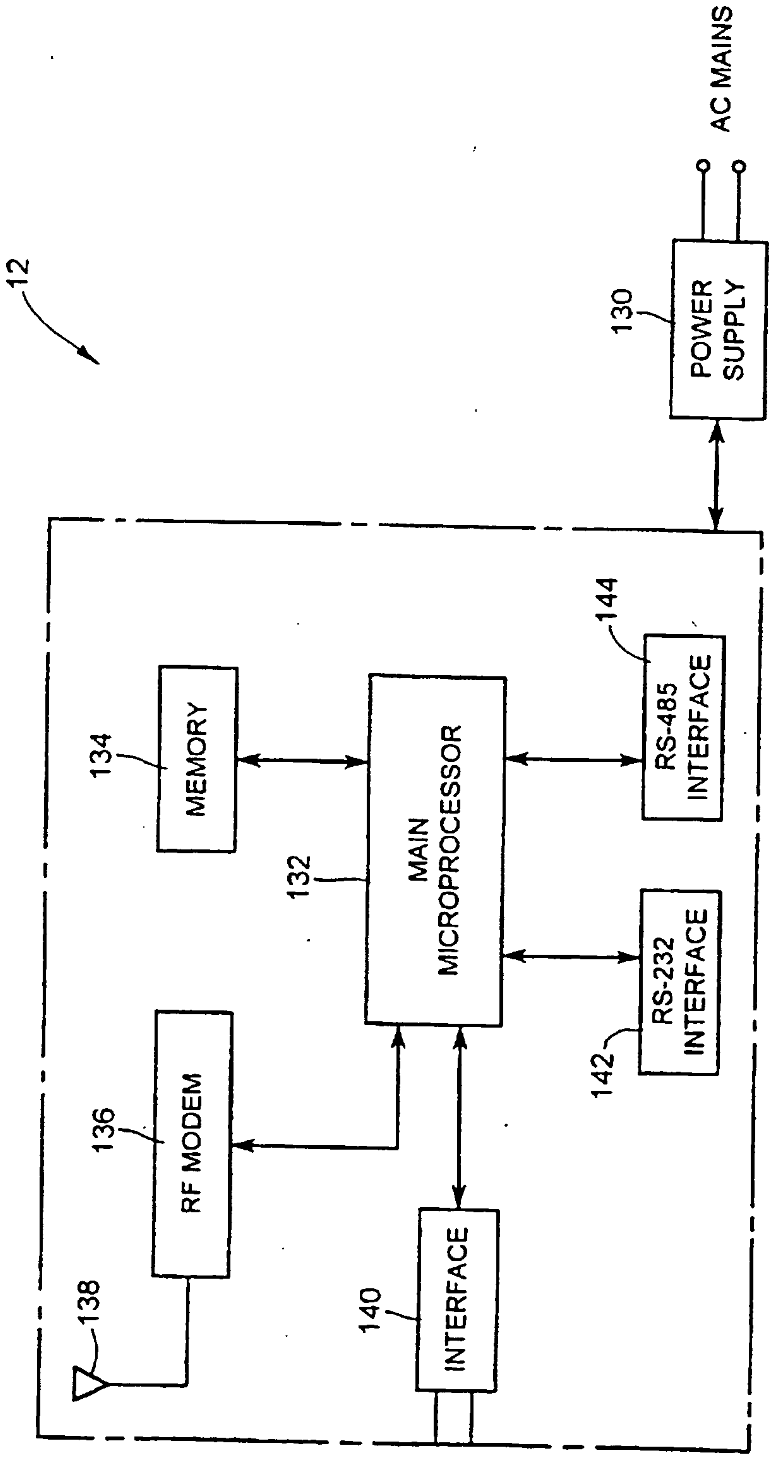

AC MAINS
12
130
POWER SUPPLY
144
RS-485 INTERFACE
134
MEMORY
132
MAIN MICROPROCESSOR
RS-232 INTERFACE
142
136
RF MODEM
138
140
INTERFACE

FIG. 6

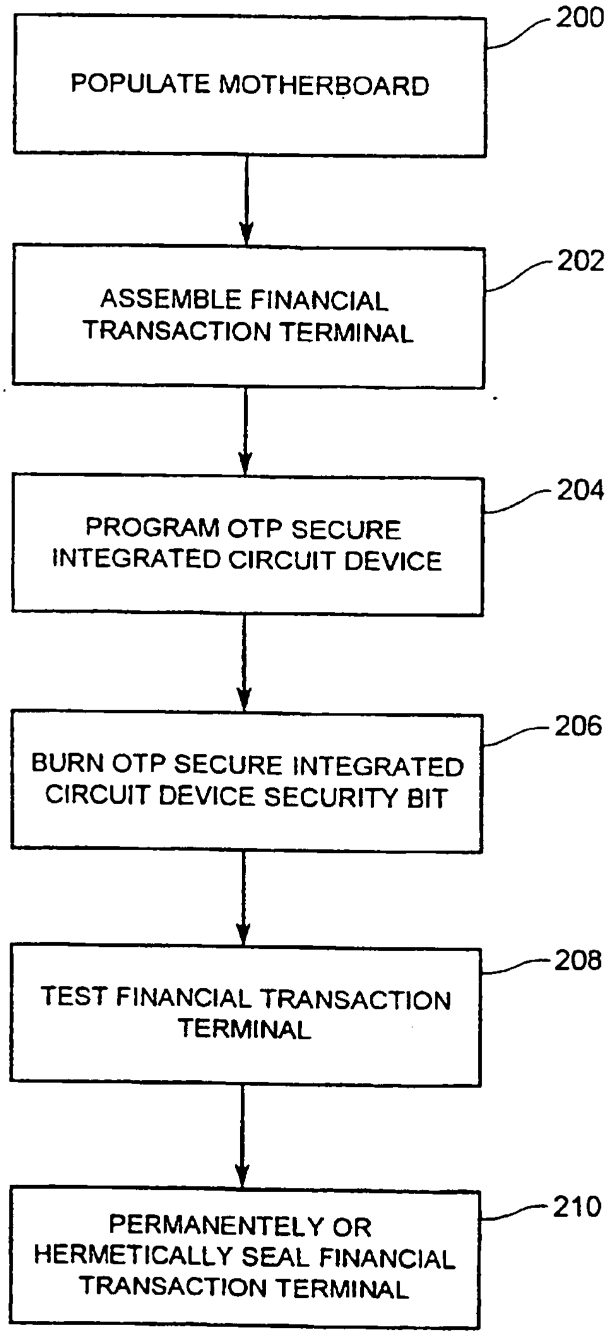

POPULATE MOTHERBOARD
200
ASSEMBLE FINANCIAL TRANSACTION TERMINAL
202
PROGRAM OTP SECURE INTEGRATED CIRCUIT DEVICE
204
BURN OTP SECURE INTEGRATED CIRCUIT DEVICE SECURITY BIT
206
TEST FINANCIAL TRANSACTION TERMINAL
208
PERMANENTELY OR HERMETICALLY SEAL FINANCIAL TRANSACTION TERMINAL
210

FIG. 7

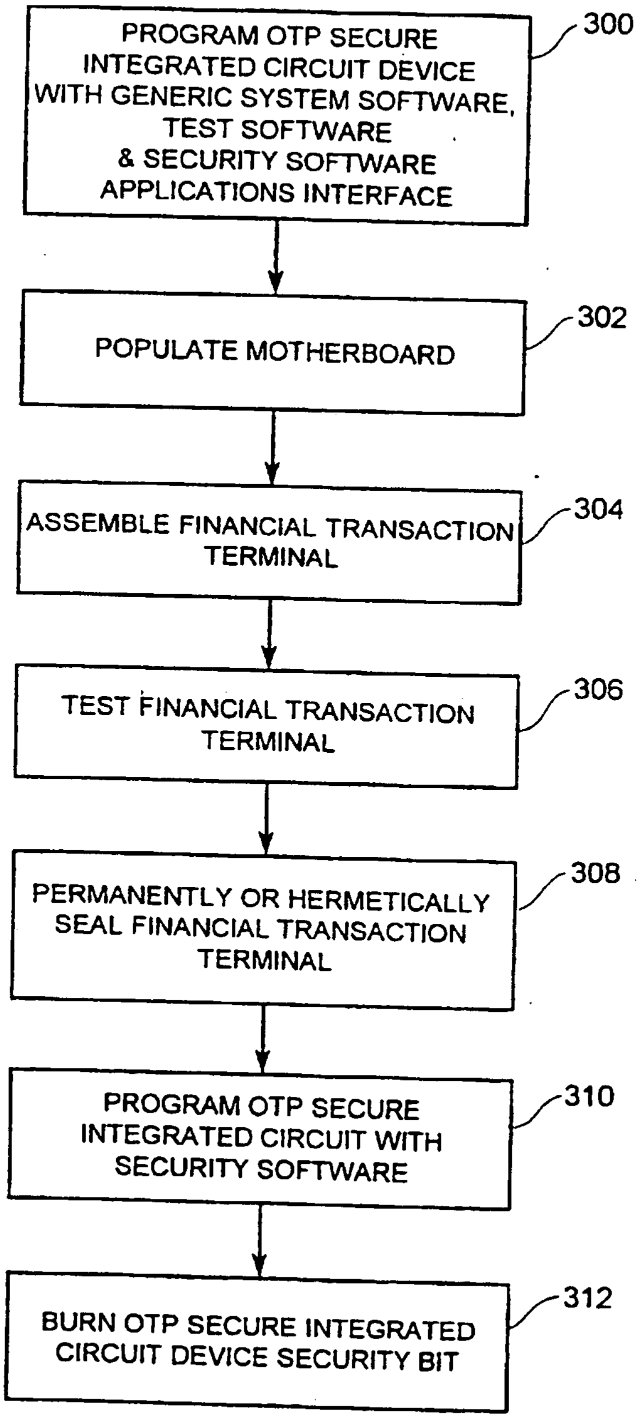

PROGRAM OTP SECURE INTEGRATED CIRCUIT DEVICE WITH GENERIC SYSTEM SOFTWARE, TEST SOFTWARE & SECURITY SOFTWARE APPLICATIONS INTERFACE
300
POPULATE MOTHERBOARD
302
ASSEMBLE FINANCIAL TRANSACTION TERMINAL
304
TEST FINANCIAL TRANSACTION TERMINAL
306
PERMANENTLY OR HERMETICALLY SEAL FINANCIAL TRANSACTION TERMINAL
308
PROGRAM OTP SECURE INTEGRATED CIRCUIT WITH SECURITY SOFTWARE
310
BURN OTP SECURE INTEGRATED CIRCUIT DEVICE SECURITY BIT
312

FIG. 8

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
G07F 7/08

A3

(11) International Publication Number: **WO 98/14915**

(43) International Publication Date: 9 April 1998 (09.04.98)

(21) International Application Number: PCT/CA97/00717

(22) International Filing Date: 30 September 1997 (30.09.97)

(30) Priority Data:

60/027,781	1 October 1996 (01.10.96)	US
08/821,732	20 March 1997 (20.03.97)	US

(71) Applicant: OMEGA DIGITAL DATA INC. [CA/CA]; 8100 Keele Street, Concord, Ontario L4K 2A3 (CA).

(72) Inventor: COVELEY, Michael; 6 Fairview Avenue, Richmond Hill, Ontario L4C 6L2 (CA).

(74) Agents: RUSTON, David, A. et al.; 6th floor, 330 University Avenue, Toronto, Ontario M5G 1R7 (CA).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

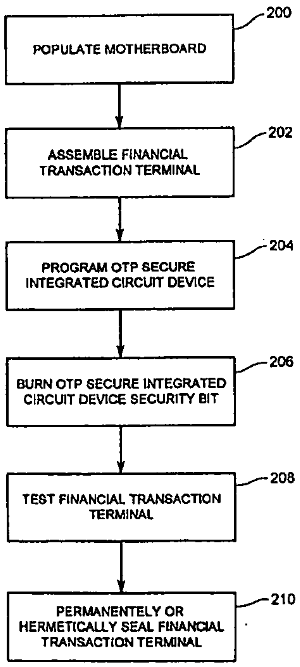
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
4 June 1998 (04.06.98)

(54) Title:. A METHOD OF ASSEMBLING AND PROGRAMMING A SECURE PERSONAL IDENTIFICATION NUMBER ENTRY DEVICE

(57) Abstract

A method of assembling and programming a secure personal identification number entry device is disclosed whereby the secure personal identification number entry device is programmed with security software including an encryption algorithm by way of an external port on the secure personal identification number entry device after the secure personal identification number device has been fully assembled.


200
POPULATE MOTHERBOARD
202
ASSEMBLE FINANCIAL TRANSACTION TERMINAL
204
PROGRAM OTP SECURE INTEGRATED CIRCUIT DEVICE
206
BURN OTP SECURE INTEGRATED CIRCUIT DEVICE SECURITY BIT
208
TEST FINANCIAL TRANSACTION TERMINAL
210
PERMANENTELY OR HERMETICALLY SEAL FINANCIAL TRANSACTION TERMINAL

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

In .ational Application No
PCT/CA 97/00717

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/08

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 456 548 A (DASSAULT ELECTRONIQUE) 13 November 1991 see claim 1; figures 1,3 ---	1-11
A	US 5 371 797 A (BOCINSKY JR RONALD V) 6 December 1994 see claim 1; figure 2 ---	1-11
A	US 5 208 446 A (MARTINEZ JERRY R) 4 May 1993 see claim 1; figures 1,4 ---	1-11
A	"PORTABLE SELF-CHECKOUT RETAIL SYSTEM" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35, no. 1A, 1 June 1992, pages 315-318, XP000308880 --- -/--	1-11

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of theinternational search 6 April 1998	Date of mailing of the international search report 16/04/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Kirsten, K

INTERNATIONAL SEARCH REPORT

Ir, .ational Application No
PCT/CA 97/00717

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 484 198 A (SAGEM) 6 May 1992 see claim 1; figure 1 ---	1-11
A	WO 94 11849 A (VATANEN HARRI TAPANI) 26 May 1994 see claim 1; figure 1 ---	1-11
A	EP 0 718 805 A (NEWS DATACOM LTD) 26 June 1996 see claim 1; figure 1 ---	1-11
A	WO 95 20195 A (DYNAMIC DATA SYSTEMS PTY LTD ;JEWELL RAIMONDE VICTOR IVAN (AU); EL) 27 July 1995 see claim 1; figures 3,4 -----	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 97/00717

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0456548 A	13-11-91	FR 2661998 A	15-11-91
		AT 124157 T	15-07-95
		DE 69110544 D	27-07-95
		DE 69110544 T	07-03-96
		FI 912215 A	11-11-91
		NO 180507 B	20-01-97
US 5371797 A	06-12-94	NONE	
US 5208446 A	04-05-93	CA 2091640 A	16-09-94
		GB 2276258 A,B	21-09-94
		US 5334824 A	02-08-94
		DE 4330254 A	30-06-94
		JP 7093411 A	07-04-95
EP 0484198 A	06-05-92	FR 2668629 A	30-04-92
		JP 4264968 A	21-09-92
		US 5387784 A	07-02-95
WO 9411849 A	26-05-94	FI 925135 A	12-05-94
		FI 934995 A	12-05-94
		AT 159602 T	15-11-97
		DE 69314804 D	27-11-97
		DE 69314804 T	12-02-98
		EP 0669031 A	30-08-95
		NO 951814 A	09-05-95
EP 0718805 A	26-06-96	NONE	
WO 9520195 A	27-07-95	AU 6641794 A	08-08-95
		CA 2181999 A	27-07-95
		CN 1142871 A	12-02-97
		EP 0741884 A	13-11-96
		JP 9507719 T	05-08-97
		NZ 265896 A	26-07-96